# INVARIANTS OF THE DIHEDRAL GROUP $D_{2p}$ IN CHARACTERISTIC TWO

MARTIN KOHLS AND MÜFİT SEZER

ABSTRACT. We consider finite dimensional representations of the dihedral group $D_{2p}$ over an algebraically closed field of characteristic two where $p$ is an odd integer and study the degrees of generating and separating polynomials in the corresponding ring of invariants. We give an upper bound for the degrees of the polynomials in a minimal generating set that does not depend on $p$ when the dimension of the representation is sufficiently large. We also show that $p + 1$ is the minimal number such that the invariants up to that degree always form a separating set. As well, we give an explicit description of a separating set when $p$ is prime.

## 1. INTRODUCTION

Let $V$ be a finite dimensional representation of a group $G$ over an algebraically closed field $F$. There is an induced action of $G$ on the algebra of polynomial functions $F[V]$ on $V$ that is given by $g(f) = f \circ g^{-1}$ for $g \in G$ and $f \in F[V]$. Let $F[V]^G$ denote the ring of invariant polynomials in $F[V]$. One of the main goals in invariant theory is to determine $F[V]^G$ by computing the generators and the relations. One may also study subsets in $F[V]^G$ that separate the orbits just as well as the full invariant ring. A set $A \subseteq F[V]^G$ is said to be separating for $V$ if for any pair of vectors $u, w \in V$, we have: If $f(u) = f(w)$ for all $f \in A$, then $f(u) = f(w)$ for all $f \in F[V]^G$. There has been a particular rise of interest in separating invariants following the text book [1]. Over the last decade there has been an accumulation of evidence that demonstrates that separating sets are better behaved and enjoy many properties that make them easier to obtain. For instance, explicit separating sets are given for all modular representations of cyclic groups of prime order in [8]. Meanwhile generating sets are known only for very limited cases for the invariants of these representations. In addition to attracting attention in their own right separating invariants can be also used as a stepping stone to build up generating invariants, see [2]. For more background and motivation on separating invariants we direct the reader to [1] and [4].

In this paper we study the invariants of the dihedral group $D_{2p}$ over a field of characteristic two where $p$ is an odd integer. The invariants of dihedral groups in characteristic zero have been worked out by Schmid in [7] where she sharpened Noether's bound for non-cyclic groups. Specifically, among other things, she proved that the invariant ring $\boldsymbol{C}[V]^{D_{2p}}$ is generated by polynomials of degree at most $p+1$.

1

Obtaining explicit generators or even sharp degree bounds is much more difficult when the order of the group is divisible by the characteristic of the field. The main difficulty is that the degrees of the generators grow unboundedly as the dimension of the representation increases. Recently, Symonds [9] established that $F[V]^G$ is generated by invariants of degree at most $(\dim V)(|G| - 1)$ for any representation $V$ of any group $G$. In section 1 we improve Symonds' bound considerably for $D_{2p}$ in characteristic two. The bound we obtain is about half of $\dim(V)$ and it does not depend on $p$ if the dimension of the part of $V$ where $D_{2p}$ does not act like its factor group $\mathbf{Z}/2\mathbf{Z}$ is large enough. In section 2 we turn our attention to separating invariants for these representations. The maximal degree of an element in the generating set for the regular representation provides an upper bound for the degrees of separating invariants. We build on this fact and our results in section 1 to compute the supremum of the degrees of polynomials in (degreewise minimal) separating sets over all representations. This resolves a conjecture in [5] positively. Then we specialize to the case where $p$ is a prime integer and describe an explicit separating set for all representations of $D_{2p}$. Our description is recursive and inductively yields a set that is "nice" in terms of constructive complexity. The set consists of invariants that are in the image of the relative transfer with respect to the subgroup of order $p$ of $D_{2p}$ together with the products of the variables over certain summands. Moreover, these polynomials depend on variables from at most three summands.

## 2. Notation and Conventions

In this section we fix the notation for the rest of the paper. Let $p \geq 3$ be an odd number and $G := D_{2p}$ be the dihedral group of order $2p$. We fix elements $\rho$ and $\sigma$ of order $p$ and $2$ respectively. Let $H$ denote the subgroup of order $p$ in $G$. Let $F$ be an algebraically closed field of characteristic two, and $\lambda \in F$ a primitive $p$-th root of unity.

**Lemma 1.** *For $0 \leq i \leq (p-1)/2$ let $W_i$ denote the two dimensional module spanned by the vectors $v_1$ and $v_2$ such that $\rho(v_1) = \lambda^{-i} v_1$, $\rho(v_2) = \lambda^i v_2$, $\sigma(v_1) = v_2$ and $\sigma(v_2) = v_1$. Then the $W_i$ together with the trivial module represent a complete list of indecomposable $D_{2p}$-modules.*

*Proof.* Let $V$ be any $D_{2p}$-module. As $p$ is odd, the action of $\rho$ is diagonalizable. For any $k \in \mathbb{Z}$, $\sigma$ induces an isomorphism of the eigenspaces of $\rho$, $\sigma : \mathrm{Eig}(\rho, \lambda^k) \xrightarrow{\sim} \mathrm{Eig}(\rho, \lambda^{-k})$. Therefore as $D_{2p}$-module, $V$ decomposes into a direct sum of $\mathrm{Eig}(\rho, 1)$ and some $W_i$'s with $1 \leq i \leq (p-1)/2$. The action of $\sigma$ on $\mathrm{Eig}(\rho, 1)$ decomposes into a direct sum of trivial summands and summands isomorphic to $W_0$. $\square$

Note that $W_i$ is faithful if and only if $i$ and $p$ are coprime. Let $V$ be a reduced $G$-module, i.e., it does not contain the trivial module as a summand. Assume that

$$V = \bigoplus_{i=1}^{r} W_{m_i} \oplus \bigoplus_{i=1}^{s} W_0,$$

where $r, s, m_i$ are integers such that $r, s \geq 0$ and $0 < m_i \leq (p-1)/2$ for $1 \leq i \leq r$. By a suitable choice of basis we identify $V = F^{2r+2s}$ with a space of $2(r+s)$-tuples $\{(a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_s, d_1, \ldots, d_s) \mid a_i, b_i, c_j, d_j \in F, \ 1 \leq i \leq r, 1 \leq j \leq s\}$ such that the projection $(a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_s, d_1, \ldots, d_s) \to (a_i, b_i) \in F^2$ is a $D_{2p}$-equivariant surjection from $V$ to $W_{m_i}$ for $1 \leq i \leq r$ and the projection

$(a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_s, d_1, \ldots, d_s) \to (c_j, d_j) \in F^2$ is a $D_{2p}$-equivariant surjection from $V$ to $W_0$ for $1 \leq j \leq s$. Let $x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_s, w_1, \ldots, w_s$ denote the corresponding basis elements in $V^*$, so we have

$$F[V] = F[x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_s, w_1, \ldots, w_s],$$

with $\sigma$ interchanging $x_i$ with $y_i$ for $1 \leq i \leq r$ and $z_j$ with $w_j$ for $1 \leq j \leq s$. The action of $\rho$ is trivial on $z_j$ and $w_j$ for $1 \leq j \leq s$. Meanwhile $\rho(x_i) = \lambda^{m_i} x_i$ and $\rho(y_i) = \lambda^{-m_i} y_i$ for $1 \leq i \leq r$.

## 3. Generating invariants

In this section we give an upper bound for the degree of generators for $F[V]^G$. Here, $p \geq 3$ is an arbitrary odd number. We continue with the introduced notation. For $1 \leq i \leq r$ and $1 \leq j \leq s$, let $a_i, b_i, c_j, d_j$ denote non-negative integers. Let $m = x_1^{a_1} \ldots x_r^{a_r} y_1^{b_1} \ldots y_r^{b_r} z_1^{c_1} \ldots z_s^{c_s} w_1^{d_1} \ldots w_s^{d_s}$ be a monomial in $F[V]$. Since $\rho$ acts on a monomial by multiplication with a scalar, all monomials that appear in a polynomial in $F[V]^G$ are invariant under the action of $\rho$. For a monomial $m$ that is invariant under the action of $\rho$, we let $o(m)$ denote its orbit sum, i.e. $o(m) = m$ if $m \in F[V]^G$ and $o(m) = m + \sigma(m)$ if $m \in F[V]^\rho \setminus F[V]^G$. As $\sigma$ permutes the monomials, we have the following:

**Lemma 2.** *Let $M$ denote the set of monomials of $F[V]$. $F[V]^G$ is spanned as a vector space by orbit sums of $\rho$-invariant monomials, i.e. by the set*

$$\{o(m) : m \in M^\rho\} = \{m + \sigma(m) : m \in M^\rho\} \cup \{m : m \in M^G\}.$$

Let $f \in F[V]_+^G$. We call $f$ expressible if $f$ is in the algebra generated by the invariants whose degrees are strictly smaller than the degree of $f$.

**Lemma 3.** *Let $m = x_1^{a_1} \ldots x_r^{a_r} y_1^{b_1} \ldots y_r^{b_r} z_1^{c_1} \ldots z_s^{c_s} w_1^{d_1} \ldots w_s^{d_s} \in M^\rho$ such that $o(m)$ is not expressible. Then $\sum_{1 \leq j \leq s} (c_j + d_j) \leq s$.*

*Proof.* Assume by contradiction that $\sum_{1 \leq j \leq s} (c_j + d_j) > s$. Pick an integer $1 \leq j \leq s$ such that $c_j + d_j \geq 2$. If both $c_j$ and $d_j$ are non-zero, then $m$ is divisible by the invariant $z_j w_j$. It follows that $o(m)$ is divisible by $z_j w_j$, hence $o(m)$ is expressible. Now assume $c_j \geq 2$ and $d_j = 0$. Note that $m/z_j \in M^\rho$. We consider the product

$$o(z_j) o(m/z_j) = (z_j + w_j)(m/z_j + \sigma(m)/w_j) = o(m) + (mw_j/z_j + \sigma(m)z_j/w_j).$$

As $mw_j/z_j$ is divisible by $z_j w_j$ (because $m$ is divisible by $z_j^2$), the invariant $f := mw_j/z_j + \sigma(m)z_j/w_j$ is divisible by $z_j w_j$. Hence $o(m) = o(z_j)o(m/z_j) + f$ is expressible. The case $c_j = 0$ and $d_j \geq 2$ is handled similarly. $\square$

**Theorem 4.** *$F[V]^G$ is generated by invariants of degree at most $s + \max\{r, p\}$.*

*Proof.* By Lemma 2 it suffices to show that $o(m)$ is expressible for any monomial $m = x_1^{a_1} \ldots x_r^{a_r} y_1^{b_1} \ldots y_r^{b_r} z_1^{c_1} \ldots z_s^{c_s} w_1^{d_1} \ldots w_s^{d_s} \in M^\rho$ of degree bigger than or equal to $s + \max\{r, p\} + 1$. Also by the previous lemma we may assume that $\sum_{1 \leq j \leq s} (c_j + d_j) \leq s$. But then $t := \sum_{1 \leq i \leq r} (a_i + b_i) \geq \max\{r, p\} + 1 \geq r + 1$, so we may take $a_1 + b_1 \geq 2$. As before, not both of $a_1$ and $b_1$ are non-zero because otherwise $o(m)$ is divisible by the invariant polynomial $x_1 y_1$ and so is expressible. So without loss of generality we assume that $a_1 \geq 2$, $b_1 = 0$. Let $\kappa_F$ denote the character group of $H$, whose elements are group homomorphisms from $H$ to $F^*$. Note that $\kappa_F \cong H$. For $1 \leq i \leq r$, let $\kappa_i \in \kappa_F$ denote the character corresponding to the action of

$H$ on $x_i$. By construction the character corresponding to the action on $y_i$ is $-\kappa_i$. Since $\rho(m) = m$ we have $\sum_{1 \leq i \leq r}(a_i\kappa_i - b_i\kappa_i) = 0$. This is an equation in a cyclic group of order $p$ that contains at least $t \geq p + 1$ (not distinct) summands. Since $a_1 \geq 2$, [7, Proposition 7.7] applies and we get non-negative integers $a_i' \leq a_i$ and $b_i' \leq b_i$ for $1 \leq i \leq r$ with $0 < a_1' < a_1$ satisfying $\sum_{1 \leq i \leq r}(a_i'\kappa_i - b_i'\kappa_i) = 0$. Hence $m_1 := x_1^{a_1'} \ldots x_r^{a_r'} y_1^{b_1'} \ldots y_r^{b_r'} z_1^{c_1} \ldots z_s^{c_s} w_1^{d_1} \ldots w_s^{d_s}$ is $\rho$-invariant. Thus $m_2 := m/m_1$ is also $\rho$-invariant. Since $0 < a_1' < a_1$, both $m_1$ and $m_2$ are divisible by $x_1$. Now consider

$$(m_1 + \sigma(m_1))(m_2 + \sigma(m_2)) = o(m) + (m_1\sigma(m_2) + \sigma(m_1)m_2).$$

As $m_1\sigma(m_2)$ is divisible by $x_1y_1$, so is $f := (m_1\sigma(m_2) + \sigma(m_1)m_2)$. It follows that $o(m) = (m_1 + \sigma(m_1))(m_2 + \sigma(m_2)) + f$ is expressible. $\qquad\square$

*Remark* 5. Assume that $V = W_i$ for some $1 \leq i \leq (p-1)/2$ such that $i$ and $p$ are coprime and set $x = x_1$ and $y = y_1$. Then by the previous theorem $F[V]^G$ is generated by invariants of degree at most $p$. But the monomials in $M^\rho$ of degree strictly less than $p$ are all divisible by $xy \in M^G$. Furthermore, the only monomials in $M^\rho$ of degree $p$ are $x^p$ and $y^p$, so it follows from Lemma 2 that $F[V]^G = F[x^p + y^p, xy]$.

## 4. Separating invariants

For a finite group $G$ (and a fixed field $F$), let $\beta_{\mathrm{sep}}(G)$ denote the smallest number $d$ such that for any representation $V$ of $G$ there exists a separating set of invariants of degree $\leq d$.

**Theorem 6.** *For an algebraically closed field $F$ of characteristic 2 and $p \geq 3$ odd, we have $\beta_{\mathrm{sep}}(D_{2p}) = p + 1$.*

Note that in [5, Proposition 10 and Example 2], bounds for $\beta_{\mathrm{sep}}(D_{2p})$ are given only in characteristics $\neq 2$, and the theorem above was conjectured for $p$ an odd prime. For example by [5], when $p$ is an odd prime and equals the characteristic of $F$, then $\beta_{\mathrm{sep}}(D_{2p^r}) = 2p^r$ for any $r \geq 1$.

*Proof.* We look at the regular representation $V_{\mathrm{reg}} := FG$, which decomposes into $V_{\mathrm{reg}} = \bigoplus_{i=1}^{\frac{p-1}{2}} W_i \oplus \bigoplus_{i=1}^{\frac{p-1}{2}} W_i \oplus W_0$. This can be seen by considering the action of $G$ on the basis of $FG$ consisting of the elements $v_k := \sum_{j=0}^{p-1} \lambda^{kj}\rho^j$ and $w_k := \sigma(v_k)$ for $k = 0, \ldots, p-1$, where $\lambda$ is a primitive $p$th root of unity. Then $\rho(v_k) = \lambda^{-k}v_k$, $\rho(w_k) = \sigma\rho^{-1}v_k = \lambda^k w_k$, and $\sigma$ interchanges $v_k$ and $w_k$. It follows that $\langle v_k, w_k \rangle \cong W_k$ if $0 \leq k \leq \frac{p-1}{2}$ and $\langle v_k, w_k \rangle \cong W_{p-k}$ if $\frac{p+1}{2} \leq k \leq p - 1$.

By Theorem 4, $F[V_{\mathrm{reg}}]^G$ is generated by invariants of degree $\leq 1 + \max\{p, 2\frac{p-1}{2}\} = 1 + p$. Hence $\beta_{\mathrm{sep}}(G) \leq p + 1$ by [3, Corollary 3.11] (see also [5, Proposition 3]). Note that for $p$ a prime, this follows constructively from Theorem 7. To prove the reverse inequality, consider $V := W_1 \oplus W_0$. We use the notation of section 2, so $F[V] = F[x, y, z, w]$ (omitting indices since $r = s = 1$) and look at the points $v_1 := (0, 1, 1, 0)$ and $v_2 := (0, 1, 0, 1)$ of $V$. They can be separated by the invariant $zx^p + wy^p$. Assume they can be separated by an invariant of degree less or equal than $p$. By Lemma 2, $F[V]^G$ is generated by invariant monomials $m \in F[V]^G$ and orbit sums $m + \sigma(m)$ of $\rho$-invariant monomials $m \in F[V]^\rho$. If such an element separates $v_1$ and $v_2$, we have $m(v_1) \neq m(v_2)$ or $(m + \sigma m)(v_1) \neq (m + \sigma m)(v_2)$

respectively. The latter implies $m(v_1) \neq m(v_2)$ or $\sigma(m)(v_1) \neq \sigma(m)(v_2)$. Replacing $m$ by $\sigma(m)$ if necessary, we thus have a $\rho$-invariant monomial $m$ separating $v_1, v_2$ of degree $\leq p$. Therefore, $x$ does not appear in $m$, so $m = y^a z^b w^c$. First assume $a = 0$. If $b = c$, then $m$ is $G$-invariant, and does not separate $v_1, v_2$. If $b \neq c$, then $m$ is not $G$-invariant, and $m + \sigma(m) = z^b w^c + z^c w^b$ does not separate $v_1, v_2$. So $a > 0$. As $m$ is $\rho$-invariant, we have $a \geq p$. Since $\deg m \leq p$, we have $a = p$ and $b = c = 0$. Then $m + \sigma(m) = y^p + x^p$ does not separate $v_1, v_2$. We have a contradiction. □

Theorem 6 gives an upper bound for the degrees of polynomials in a separating set. In the following, under the additional assumption that $p > 2$ is a prime, we construct a separating set explicitly. We use again the notation of section 2. We assume that $V$ is a faithful $G$-module. In particular we have $r \geq 1$. Let $1 \leq i \leq r - 1$ be arbitrary. Since the action of $\rho$ is non-trivial on each of the variables $x_r, y_1, \ldots, y_{r-1}$ there exists a positive integer $n_i \leq p - 1$ such that $x_r y_i^{n_i}$ and $x_r x_i^{p-n_i}$ are invariant under the action of $\rho$. We thus get invariants

$$f_i := x_r y_i^{n_i} + y_r x_i^{n_i}, \quad g_i := x_r x_i^{p-n_i} + y_r y_i^{p-n_i} \in F[V]^G \quad \text{for } i = 1, \ldots, r - 1.$$

For $1 \leq i \leq r - 1$ and $1 \leq j \leq s$ we also define

$$f_{i,j} := x_r y_i^{n_i} z_j + y_r x_i^{n_i} w_j, \quad h_j := x_r^p z_j + y_r^p w_j \in F[V]^G.$$

Set $V' = \bigoplus_{i=1}^{r-1} W_{m_i} \oplus \bigoplus_{i=1}^{s} W_0$.

**Theorem 7.** *Let $p > 2$ be a prime. Let $S$ be a separating set for $V'$. Then $S$ together with the set*

$$T = \{x_r y_r, x_r^p + y_r^p, f_i, g_i, f_{i,j}, h_j \mid 1 \leq i \leq r - 1, \ 1 \leq j \leq s\}$$

*of invariant polynomials is a separating set for $V$.*

Note that a separating set for $\bigoplus_{i=1}^{s} W_0$ is given in [8].

*Proof.* We have a surjection $V \to V' : (a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_s, d_1, \ldots, d_s) \to (a_1, \ldots, a_{r-1}, b_1, \ldots, b_{r-1}, c_1, \ldots, c_s, d_1, \ldots, d_s)$ which is $G$-equivariant. Therefore by [6, Theorem 1] it suffices to show that the polynomials in $T$ separate any pair of vectors $v_1$ and $v_2$ in different $G$-orbits that agree everywhere except $r$-th and $2r$-th coordinates. So we take $v_1 = (a_1, \ldots, a_r, b_1, \ldots, b_r, c_1, \ldots, c_s, d_1, \ldots, d_s)$ and $v_2 = (a_1, \ldots, a_{r-1}, a_r', b_1, \ldots, b_{r-1}, b_r', c_1, \ldots, c_s, d_1, \ldots, d_s)$. Assume by way of contradiction that no polynomial in $T$ separates $v_1$ and $v_2$. Since $\{x_r y_r, x_r^p + y_r^p\} \subseteq T$ is a separating set for $W_{m_r}$ by Remark 5, we may further take that $(a_r, b_r)$ and $(a_r', b_r')$ are in the same $G$-orbit. Consequently, there are two cases.

First we assume that there exists an integer $t$ such that $(a_r', b_r') = \rho^t(a_r, b_r)$. Hence $a_r' = \lambda^{-tm_r} a_r$ and $b_r' = \lambda^{tm_r} b_r$. Set $c := \lambda^{-tm_r}$. Notice that $a_r$ and $b_r$ can not be zero simultaneously because otherwise $v_1 = v_2$. Without loss of generality we take $a_r \neq 0$. Also if $a_i = b_i = 0$ for all $1 \leq i \leq r - 1$ then we have $\rho^t(v_1) = v_2$, hence $r > 1$ and there is an index $1 \leq q \leq r - 1$ such that at least one of $a_q$ or $b_q$ is non-zero. We show in fact both $a_q$ and $b_q$ are non-zero together with $b_r$. First assume that $a_q \neq 0$. If one of $b_q$ or $b_r$ is zero, then $g_q(v_1) = a_r a_q^{p-n_q}$ and $g_q(v_2) = c a_r a_q^{p-n_q}$. This yields a contradiction because $g_q(v_1) = g_q(v_2)$. Next assume that $b_q \neq 0$. If one of $a_q$ or $b_r$ is zero then $f_q(v_1) = a_r b_q^{n_q}$ and $f_q(v_2) = c a_r b_q^{n_q}$, yielding a contradiction again. In fact, applying the same argument using the invariant $g_i$ (or $f_i$) shows that for $1 \leq i \leq r - 1$ we have: $a_i \neq 0$ if and only if $b_i \neq 0$. We

claim that $a_i^p = b_i^p$ for $1 \le i \le r-1$. Clearly we may assume $a_i \neq 0$. From $f_i(v_1) = f_i(v_2)$ we get $(1+c)a_r b_i^{n_i} = (1+c^{-1})b_r a_i^{n_i}$. Similarly from $g_i(v_1) = g_i(v_2)$ we have $(1+c)a_r a_i^{p-n_i} = (1+c^{-1})b_r b_i^{p-n_i}$. It follows that

$$c^{-1} = \frac{a_r b_i^{n_i}}{b_r a_i^{n_i}} = \frac{a_r a_i^{p-n_i}}{b_r b_i^{p-n_i}}.$$

This establishes the claim. For $1 \le i \le r-1$, let $e_i$ denote the smallest non-negative integer such that $b_i = \lambda^{e_i} a_i$. We also have $b_r = c\lambda^{e_i n_i} a_r$ provided $a_i \neq 0$. We now show that $c_j = d_j$ for all $1 \le j \le s$. From $f_{q,j}(v_1) = f_{q,j}(v_2)$ we have $c_j a_r b_q^{n_q} + d_j b_r a_q^{n_q} = c c_j a_r b_q^{n_q} + c^{-1} d_j b_r a_q^{n_q}$. Putting $b_q = \lambda^{e_q} a_q$ and $b_r = c\lambda^{e_q n_q} a_r$ we get $c_j a_r \lambda^{e_q n_q} a_q^{n_q} + d_j c \lambda^{e_q n_q} a_r a_q^{n_q} = c c_j a_r \lambda^{e_q n_q} a_q^{n_q} + c^{-1} d_j c a_r \lambda^{e_q n_q} a_q^{n_q}$ which gives $c_j + c d_j = c c_j + d_j$. This implies $c_j = d_j$ as desired because $1 + c \neq 0$. We now have $v_1 = (a_1, \ldots, a_r, \lambda^{e_1} a_1, \ldots, \lambda^{e_{r-1}} a_{r-1}, c\lambda^{e_q n_q} a_r, c_1, \ldots, c_s, c_1, \ldots, c_s)$ and $v_2 = (a_1, \ldots, a_{r-1}, c a_r, \lambda^{e_1} a_1, \ldots, \lambda^{e_{r-1}} a_{r-1}, \lambda^{e_q n_q} a_r, c_1, \ldots, c_s, c_1, \ldots, c_s)$. Since $0 < m_r < p$, there exists an integer $0 \le h \le p-1$ such that $-h m_r + e_q n_q \equiv 0$ mod $p$. We obtain a contradiction by showing that $\rho^h \sigma(v_1) = v_2$. Since the action of $\rho$ on the last $2s$ coordinates is trivial it suffices to show that $\lambda^{-h m_i} b_i = a_i$ for $1 \le i \le r-1$ and $\lambda^{-h m_r} b_r = c a_r$. Hence we need to show $-h m_i + e_i \equiv 0$ mod $p$ for $1 \le i \le r-1$ when $a_i \neq 0$, and $-h m_r + e_q n_q \equiv 0$ mod $p$. The second equality follows by the choice of $h$. So assume that $1 \le i \le r-1$ and $a_i \neq 0$. We have $m_r - n_i m_i \equiv 0$ mod $p$ because $x_r y_i^{n_i}$ is invariant under the action of $\rho$. It follows that $e_q n_q - h n_i m_i \equiv 0$ mod $p$. But since $e_i n_i \equiv e_q n_q$ (as $b_r = c\lambda^{e_i n_i} a_r = c\lambda^{e_q n_q} a_r$) we have $n_i(e_i - h m_i) \equiv 0$ mod $p$. Since $n_i$ is non-zero modulo $p$ we have $e_i - h m_i \equiv 0$ mod $p$ as desired.

Next we consider the case $(a'_r, b'_r) = \rho^t \sigma(a_r, b_r)$ for some integer $t$. Hence $a'_r = \lambda^{-t m_r} b_r$ and $b'_r = \lambda^{t m_r} a_r$. Set $c := \lambda^{-t m_r}$. As in the first case one of $a_r$ or $b_r$ is non-zero, so without loss of generality we take $a_r \neq 0$. As $h_j(v_1) = h_j(v_2)$ for $1 \le j \le s$, we get $(a_r^p + a_r'^p)c_j = (b_r^p + b_r'^p)d_j$, which implies $(a_r^p + b_r^p)c_j = (a_r^p + b_r^p)d_j$. If $a_r^p = b_r^p$, we have $b_r = \lambda^l a_r$ for some $l$. Then we have $(a'_r, b'_r) = (\lambda^{-t m_r + l} a_r, \lambda^{t m_r - l} b_r) \in \langle \rho \rangle \cdot (a_r, b_r)$, so we are again in the first case. Therefore we can assume $a_r^p \neq b_r^p$, and we get $c_j = d_j$ for all $1 \le j \le s$. Now, if $a_i = b_i = 0$ for all $1 \le i \le r-1$, then $v_2 = \rho^t \sigma(v_1)$. Hence $r > 1$ and there is an index $1 \le q \le r-1$ such that at least one of $a_q$ or $b_q$ is non-zero. Let $1 \le i \le r-1$. From $f_i(v_1) = f_i(v_2)$ we get $a_r b_i^{n_i} + b_r a_i^{n_i} = c b_r b_i^{n_i} + c^{-1} a_r a_i^{n_i}$ and so $a_i^{n_i}(c^{-1} a_r + b_r) = b_i^{n_i}(a_r + c b_r)$. Note that $c^{-1} a_r + b_r \neq 0$ because otherwise $v_1 = v_2$. So we have $a_i^{n_i} = c b_i^{n_i}$. Along the same lines, from $g_i(v_1) = g_i(v_2)$ we obtain $b_i^{p-n_i} = c a_i^{p-n_i}$. It follows that $a_i^p = b_i^p$. As before, for $1 \le i \le r-1$ let $e_i$ denote the smallest non-negative integer such that $b_i = \lambda^{e_i} a_i$. We also have $c = \lambda^{-n_i e_i}$ for all $1 \le i \le r-1$ with $a_i \neq 0$. We have $v_1 = (a_1, \ldots, a_r, \lambda^{e_1} a_1, \ldots, \lambda^{e_{r-1}} a_{r-1}, b_r, c_1, \ldots, c_s, c_1, \ldots, c_s)$ and $v_2 = (a_1, \ldots a_{r-1}, c b_r, \lambda^{e_1} a_1, \ldots, \lambda^{e_{r-1}} a_{r-1}, c^{-1} a_r, c_1, \ldots, c_s, c_1, \ldots, c_s)$. We finish the proof by demonstrating that $v_1$ and $v_2$ are in the same orbit. Since $0 < m_r < p$, there exists an integer $0 \le h \le p-1$ such that $\lambda^{-h m_r} = c$. Equivalently, $-h m_r + e_q n_q \equiv 0$ mod $p$. We claim that $\rho^h \sigma(v_1) = v_2$. Since $c_j = d_j$ for $1 \le j \le s$ and the action of $\rho$ on the last $2s$ coordinates is trivial we just need to show that $\lambda^{-h m_i} b_i = a_i$ for $1 \le i \le r-1$ and $\lambda^{-h m_r} b_r = c b_r$. Since the last equation is taken care of by construction we just need to show $-h m_i + e_i \equiv 0$ mod $p$ for $1 \le i \le r-1$ when $a_i \neq 0$. We get $e_i n_i \equiv e_q n_q$ from $c = \lambda^{-e_i n_i} = \lambda^{-e_q n_q}$. Now the proof can be finished by exactly the same argument as in the first case.  □

## References

[1] Harm Derksen and Gregor Kemper. *Computational invariant theory.* Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[2] Harm Derksen and Gregor Kemper. Computing invariants of algebraic groups in arbitrary characteristic. *Adv. Math.*, 217(5):2089–2129, 2008.

[3] Jan Draisma, Gregor Kemper, and David Wehlau. Polarization of separating invariants. *Canad. J. Math.*, 60(3):556–571, 2008.

[4] G. Kemper. Separating invariants. *J. Symbolic Comput.*, 44:1212–1222, 2009.

[5] Martin Kohls and Hanspeter Kraft. On degree bounds for separating invariants. *Mathematical Research Letters, to appear*, 2010.

[6] Martin Kohls and Müfit Sezer. Separating invariants for the klein four group and the cyclic groups. *arXiv:1007.5197*, 2010.

[7] Barbara J. Schmid. Finite groups and invariant theory. In *Topics in invariant theory (Paris, 1989/1990)*, volume 1478 of *Lecture Notes in Math.*, pages 35–66. Springer, Berlin, 1991.

[8] Müfit Sezer. Constructing modular separating invariants. *J. Algebra*, 322(11):4099–4104, 2009.

[9] P. Symonds. On the Castelnuovo-Mumford regularity of rings of polynomial invariants. *Preprint, available at http://www.maths.manchester.ac.uk/ pas/preprints/*, 2009.

TECHNISCHE UNIVERSITÄT MÜNCHEN, ZENTRUM MATHEMATIK-M11, BOLTZMANNSTRASSE 3, 85748 GARCHING, GERMANY
*E-mail address*: `kohls@ma.tum.de`

DEPARTMENT OF MATHEMATICS, BILKENT UNIVERSITY, ANKARA 06800 TURKEY
*E-mail address*: `sezer@fen.bilkent.edu.tr`